March 4, 2014
*Via electronic mail only*

Hon. Desley Brooks (dbrooks@oaklandnet.com)
Hon. Noel Gallo (ngallo@oaklandnet.com)
Hon. Rebecca Kaplan (atlarge@oaklandnet.com)
Hon. Pat Kernighan (Pkernighan@oaklandnet.com)
Hon. Lynette McElhaney (lmcelhaney@oaklandnet.com)
Hon. Dan Kalb (dkalb@oaklandnet.com)
Hon. Larry Reid (lreid@oaklandnet.com)
Hon. Libby Schaaf (lschaaf@oaklandnet.com)
Oakland City Council
1 Frank H. Ogawa Plaza
Oakland, CA 94612

re: Domain Awareness Center, Phase 2 Contract Award

Dear Honorable Members of the Oakland City Council,

The American Civil Liberties Union of Northern California writes in regard to Item 14 on the March 4, 2014 Agenda of the City Council, pertaining to the Oakland Domain Awareness Center. Once again, we urge you not to approve the resolution proposed by staff. We reiterate our previously expressed grave concerns about the DAC and its enormous potential for abuse. In this letter, we address three further points. *First*, while we urge you not to grant the DAC any further approvals at this time, numerous City Council members at the last Council meeting expressed interest in a Port-only approach. The proposed resolution fails to implement that approach. *Second*, the City Council expressly instructed staff to provide additional information about the component systems of the DAC so that the Council could decide which systems are and are not Port related. Yet the staff report (filed February 27, 2014) once again fails to provide the Council with the basic factual information it needs to engage in oversight. This omission allows staff to usurp what is fundamentally the Council's policy-making prerogative of deciding what systems to include in the DAC. Unfortunately, rather than providing a balanced or complete factual account, the staff report omits essential factual and legal issues. *Third*, both the public and members of the City Council have expressed reservations about the potential for federal access to information collected and retained by the DAC. The staff report suggests that any such concerns are unfounded because "information sharing would be limited unless there is a written agreement for information sharing." (Staff Report at page 14.) The staff report entirely fails to mention that the federal government under the Patriot Act can obtain a wide array of information without such niceties as a voluntary information sharing agreement.



**AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA**
39 DRUMM STREET, SAN FRANCISCO, CA 94111 | T/415.621.2493 | F/415.255.1478 | TTY/415.863.7832 | WWW.ACLUNC.ORG

***The proposed resolution does not reflect the views of City Council members that the DAC should be limited to Port-only systems.*** Numerous City Councilmembers expressed the view at the last City Council meeting that the DAC should include only those systems that are related to the Port. The proposed resolution does not reflect that perspective.

A new City Council resolution is necessary to implement a Port-only approach because Resolution 84593, enacted last summer, authorized the inclusion of various City-based surveillance systems (such as Automated Licensed Plate Readers and City-owned cameras). If the City Council wishes to authorize a Port-only system, new resolution language is required to make clear that the previously authorized City-based systems are now not authorized for inclusion.

In addition, a new City Council resolution should specify the systems and capabilities that are authorized for inclusion and that no additional systems or capabilities may be added without express City Council authorization. The determination whether a particular system or capability is or is not Port-related reflects a policy choice. That choice should be made by the Council, not staff.

***The staff report's omission of key factual and legal information interferes with the Council's ability to engage in meaningful oversight.*** Despite the Council's express instruction to staff to provide information on the component systems already included in Phase 1 and slated for inclusion in Phase 2, the staff report continues to provide insufficient information for the City Council to make an informed decision about what systems to include in the DAC. The descriptions of each component systems leaves open many unanswered questions. For example:

* **Shot spotter (Phase 1)**. The staff report's description states that Shot Spotter "detects gunfire in the City and quickly locates the incident on a map." (Staff Report at page 3.) It does not explain *how* Shot Spotter does so. While the staff report fails to explain this, Shot Spotter's website states that it detects gunshots through "[w]ide-area acoustic surveillance," which consists of "the deployment of multiple collaborative acoustic sensors through a coverage area to create a robust, redundant coverage array stretch from a single square mile up to 20 or more square miles."[1] *What type of information is recorded through this "wide-area acoustic surveillance"? How does wide-area acoustic surveillance (as distinct from the location of gun shots) help further Port security and why should it be included in the DAC?* The staff report states that "seeing the entire picture is critical to responder safety and effective response" (page 3), but this "justification" would also justify including cameras in schools and other systems that the City Council has decided to exclude from the DAC.

* **Traffic cameras (Phase 1).** The staff report states that "Traffic cameras are focused on important traffic areas in the City." (Staff Report at page 4.) *But what information do traffic cameras capture and record? Do they capture a wide swath of information that sweeps up pedestrians? Do they record information at sufficient resolution to capture the images of individuals in vehicles, record license plates, and other information that would allow identification of individuals? How does each of these capabilities further Port security?*

[1] Available at https://www.shotspotter.com/technology/wide-area-acoustic-surveillance.

* **Police and Fire CAD Data (Phase 2).** The Staff Report states that the "[s]ystem … tracks incidents/dispatches and includes all incident records and details." (Staff Report at page 6.) This sentence provides so little information that it is difficult to understand what the system is. *What is an "incident"? How does the system "track" it? And what is included in the universe of "all incident records and details"? How does access to each type of information tracked by the CAD system further Port security?* The staff report states that access to this information would allow "EOC staff to keep updated on specific incidents without tying up dispatcher's time" but this rationale is so broad (keeping EOC staff "updated") as to justify collection of all kinds of information, including information that the City Council has already decided should not be included in the DAC (such as surveillance feeds from Oakland schools).

* **Police and Fire Records Management System (Phase 2).** The Staff Report states that the Records Management System "tracks and includes case records for OPD and OFD." (Staff Report at page 6.) Again, this sentence provides so little information that it is entirely unclear what this system is and how it differs from the CAD system. *What is a "case record" within this system? Does it include all arrest records, including records of arrests that did not lead to charge or conviction? How does this system "track" such records? How does access to each type of record tracked by the RMS system (such as records of arrests that did not lead to charge or conviction) further Port security? Does DAC access to OPD arrest records comport with state law restrictions on access to criminal history information?* To the extent that the RMS includes all of OPD's arrest reports, access to this information would amount to access to comprehensive criminal history information – in effect, a "rap sheet" – about thousands of individuals, including information about arrests that did not lead to charge or conviction. State law places strict limitations on the distribution of protected rap sheet information. *See* Penal Code §13300; *International Federation of Professional and Technical Engineers, Local 21 v. Superior Court*, 42 Cal.4th 319, 339 (2007) ("Penal Code section 13300 . . . generally prohibits a local criminal justice agency, including a court, from distributing information that relates a person's criminal history"); Ops.Cal.Atty.Gen. 06-203, 12 (2006) (prosecutor may not produce in response to Public Record Act request the criminal history of an individual in the county, including all arrests and case dispositions, because the information is protected rap sheet information pursuant to Penal Code §§13300-13305). Depending on who would have access to this information through the DAC, inclusion of the RMS within the DAC may violate state law provisions governing rap sheet information.

* **Various News Feeds & Alerts (Phase 2)**. The Staff Report states that alerts "may come in via email, web feed, RSS, *or other means*." (Staff Report at page 8, emphasis added.) *What "other means" would feed into this system? Would it include social media feeds*? National Public Radio recently aired a story about new investigative tools that monitor social media feeds. *See* Martin Kaste, "As Police Monitor Social Media, Legal Lines Become Blurred," NPR (Feb. 28, 2014).[2] As Vernon Keenan, the director of the Georgia

[2] Available at http://www.npr.org/blogs/alltechconsidered/2014/02/28/284131881/as-police-monitor-social-media-legal-lines-become-blurred.

Bureau of Investigation stated, "For law enforcement to be there and to take photographs of all the participants [of a political protest] — monitoring — is not against the law, but it's not acceptable." *Id.* As a result, "Keenan requires his agents to get permission from a supervisor before they scan social media. They have to explain what they're monitoring and why." *Id.* Law enforcement monitoring of social media, especially through sophisticated new technology, raises cutting edge legal and public policy questions that need to be aired thoroughly.[3] The City Council should not inadvertently authorize the DAC to include social media monitoring without first examining and debating the issues, and allow the public to present all perspectives. If the City Council is inclined to include this system in the DAC, it should expressly clarify that only the feeds listed in the Staff Report (US Coast Guard notifications, State Warning Center, Homeland Security Information Alerts, Cal Fire Alerts, FEMA News releases, and California Dept. of Fish and Game) are included and that all other email and web feeds, including social media, are excluded.

The Staff Report also states that "[t]hese feeds will allow creation of automatic alerts of events that meet thresholds. Alerts can signal EOC staff to execute pre-written action plans specific to the event. The pre-written action plans will be embedded into the system." (Staff Report at page 8.) *What kinds of "thresholds" will the automatic alerts trigger? What are the "pre-written action plans" that will be executed?*

***The federal government can access information in the DAC under the Patriot Act.***
Various City Councilmembers and the public have repeatedly expressed concerns about the DAC in light of the Snowden revelations of pervasive NSA spying. The Staff Report suggests that concerns about federal access to information aggregated by the DAC are unfounded because "information sharing would be limited unless there is a written agreement for sharing information collected and stored by the DAC" and "information received in the DAC is considered third party information and the City of Oakland cannot provide the information unless it is the owner of the video and data." (Staff Report at 14). It is unclear why the City of Oakland would not be considered the "owner" of video or data from, for example, City Shot Spotter, City traffic cameras, or records of the City police and fire departments, all either already included in Phase 1 or slated for inclusion in Phase 2. More significantly, the Staff Report fails to acknowledge that the federal government can demand information without any information sharing agreement, a warrant, or a subpoena. Under Section 215 of the Patriot Act (codified at 50 U.S.C. §1861), the FBI can obtain secret court orders from the Foreign Intelligence Surveillance Court compelling third parties to produce "any tangible thing" that is "relevant" to foreign intelligence or terrorism investigations. Section 215 includes a "gag order" provision, such that the recipient of an order is generally prohibited from disclosing it. *See* 50 U.S.C. §1861(d). Unfortunately, involvement of the Foreign Intelligence Surveillance Court provides little assurance that the government will not use Section 215 to engage in dragnet and intrusive sweeps for information. The government has relied on Section 215 in obtaining metadata of all

[3] In December 2012, the San Francisco District Attorney issued a subpoena to Twitter seeking "tweets" of several individuals who had been arrested at a political protest. After the ACLU and Electronic Frontier Foundation filed an amicus brief urging the court to quash the subpoena, the District Attorney – in a tacit acknowledgment of the complex legal issues implicated by the subpoena – voluntarily withdrew the subpoena. *See* Xeni Jardin, "SF District Attorney withdraws subpoenas seeking Twitter users' account data," BoingBoing (Jan. 2, 2013), available at http://boingboing.net/2013/01/02/sf-district-attorney-withdraws.html.

domestic telephone calls from Verizon, as revealed by Edward Snowden last summer. *See* Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," The Guardian (June 5, 2013).[4] While the ACLU is currently challenging the constitutionality of Section 215, the statute currently remains in force.

* * *

For the foregoing reasons, we urge you not to approve the proposed resolution.

Sincerely,

Linda Lye
Staff Attorney
ACLU of Northern California

[4]Available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.